WHAT IS CLAIMED IS:

1. A computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, causes a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information; and

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria.

2. The computer program according to claim 1, causes the computer to further perform changing the setting information upon it is judged at the judging that the communication is executed by the worm, wherein

the acquiring includes acquiring the information based on the setting information after change.

3. The computer program according to claim 1, causes the computer to further perform changing the judgment criteria upon it is judged at the judging that the communication is executed by the worm, wherein

the judging includes judging whether the communication is executed by the worm based on the information acquired and the setting information after change.

4. The computer program according to claim 1, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.

5. The computer program according to claim 4, wherein the judging includes judging that a communication from a plurality of computer in the predetermined segment is executed by the worm when

a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, and

the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside.

6. The computer program according claim 1, wherein the judging includes judging that a communication from a computer that is outside the predetermined network segment is executed by the worm when

there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, and

there is an increase in number of sender addresses of the communication packets.

7. The computer program according to claim 1, wherein the judging includes outputting any one of information about a computer that performed the communication and a communication status upon it is judged that the communication is executed by the worm.

8. The computer program according to claim 1, wherein the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that is recorded in advance.

9. The computer program according to claim 1, causes the computer to perform cutting off the communication executed by the worm upon it is judged that the communication is executed by the worm.

10. The computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by stopping a process that is started by the worm.

11. The computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by making a fire wall function effective in a computer that is judged to have

a worm.

12. A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information; and

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria.

13. A method for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

acquiring information related to a traffic and a communication address of a communication packet based on setting information; and

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria.

14. A device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

an acquiring unit that acquires information related to a traffic and a communication address of a communication packet based on setting information; and

a judging unit that judges whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria.

15. The device according to claim 14, further comprising a setting changing unit that changes the setting information upon it is judged by the judging unit that the communication is executed by the worm, wherein

the acquiring unit acquires the information based on the setting information after change.

16. The device according to claim 14, further comprising a setting changing unit that changes the judgment criteria upon it is judged by the judging unit that the communication is executed by the worm, wherein

the judging unit judges whether the communication is executed by the worm based on the information acquired by the acquiring unit and the setting information after change.

17. The device according to claim 14, wherein the judging unit judges that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.

18. The device according to claim 17, wherein the judging unit judges that a communication from a plurality of computer in the predetermined segment is executed by the worm when

a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, and

the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside.

19. The device according claim 14, wherein the judging unit judges that a communication from a computer that is outside the predetermined network segment is executed by the worm when

there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, and

there is an increase in number of sender addresses of the communication packets.

20. The device according to claim 14, wherein the judging unit judges outputs any one of information about a computer that performed the communication and a communication status upon it is judged that the communication is executed by the worm.